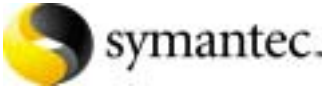
ManHunt Smart Agent for
Symantec™ Host IDS 4.1

Installation Guide



ManHunt Smart Agent for Symantec Host IDS 4.1 Installation Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Copyright Notice

Copyright © 2003 Symantec Corporation.

All Rights Reserved.

Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY. The technical documentation is being delivered to you AS-IS, and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.

No part of this publication may be copied without the express written permission of Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

Trademarks

Symantec and the Symantec logo are U.S. registered trademarks of Symantec Corporation.

Other brands and product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

SYMANTEC SOFTWARE LICENSE AGREEMENT (SMART AGENT)

SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU OR YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND THE LICENSOR. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING ON THE "AGREE" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK ON THE "I DO NOT AGREE", "NO" BUTTON, OR OTHERWISE INDICATE REFUSAL AND MAKE NO FURTHER USE OF THE SOFTWARE.

1. LICENSE.

The software and documentation that accompanies this license (collectively the "Software") is the proprietary property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, You will have certain rights to use the Software after Your acceptance of this license. This license governs any releases, revisions, or enhancements to the Software that the Licensor may furnish to You. Except as may be modified by an applicable Symantec license certificate, license coupon, or license key (each a "License Module") that accompanies, precedes, or follows this license, Your rights and obligations with respect to the use of this Software are as follows:

YOU MAY:

A. use that number of copies of the Software as have been licensed to You by Symantec under a License Module for Your internal business purposes. Your License Module shall constitute proof of Your right to make such copies. If no License Module accompanies, precedes, or follows this license, You may make one copy of the Software You are authorized to use on a single machine.

B. make one copy of the Software for archival purposes, or copy the Software onto the hard disk of Your computer and retain the original for archival purposes;

C. use each licensed copy of the Software on a single central processing unit; and

D. after written consent from Symantec, transfer the Software on a permanent basis to another person or entity, provided that You retain no copies of the Software and the transferee agrees to the terms of this license.

YOU MAY NOT:

A. copy the printed documentation which accompanies the Software;

B. sublicense, rent or lease any portion of the Software; reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;

C. use a previous version or copy of the Software after You have received a disk replacement set or an upgraded version. Upon upgrading the Software, all copies of the prior version must be destroyed;

D. use a later version of the Software than is provided herewith unless You have purchased corresponding maintenance and/or upgrade insurance or have otherwise separately acquired the right to use such later version;

E. use, if You received the software distributed on media containing multiple Symantec products, any Symantec software on the media for which You have not received a permission in a License Module; nor

F. use the Software in any manner not authorized by this license.

2. CONTENT UPDATES:

Certain Software utilize content which is updated from time to time (including but not limited to the following Software: antivirus software utilize updated virus definitions; content filtering software utilize updated URL lists; some firewall software utilize updated firewall rules; and vulnerability assessment products utilize updated vulnerability data; these updates are collectively referred to as "Content Updates"). You shall have the right to obtain Content Updates for any period for which You have purchased maintenance, except for those Content Updates which Symantec elects to make available by separate paid subscription, or for any period for which You have otherwise separately acquired the right to obtain Content Updates. Symantec reserves the right to designate specified Content Updates as requiring purchase of a separate subscription at any time and without notice to You; provided, however, that if You purchase maintenance hereunder that includes particular Content Updates on the date of purchase, You will not have to pay an additional fee to continue receiving such Content Updates through the term of such maintenance even if Symantec designates such Content Updates as requiring separate purchase. This License does not otherwise permit Licensee to obtain and use Content Updates.

3. LIMITED WARRANTY:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to You. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money You paid for the Software. Symantec does not warrant that the Software will meet Your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

4. DISCLAIMER OF DAMAGES:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO CASE SHALL SYMANTEC'S LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and

limitations set forth above will apply regardless of whether You accept the Software.

5. U.S. GOVERNMENT RESTRICTED RIGHTS:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are "Commercial Items", as that term is defined in 48 C.F.R. section 2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation", as such terms are defined in 48 C.F.R. section 252.227-7014(a)(5) and 48 C.F.R. section 252.227-7014(a)(1), and used in 48 C.F.R. section 12.212 and 48 C.F.R. section 227.7202, as applicable. Consistent with 48 C.F.R. section 12.212, 48 C.F.R. section 252.227-7015, 48 C.F.R. section 227.7202 through 227.7202-4, 48 C.F.R. section 52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec's computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014, United States of America.

6. EXPORT REGULATION:

Export, re-export of this Software is governed by the laws and regulations of the United States and import laws and regulations of certain other countries Export or re-export of Software to any entity on the Denied Parties List and other lists promulgated by various agencies of the United States Federal Government is strictly prohibited.

7. GENERAL:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the laws of England. This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Software and: (i) supersedes all prior or contemporaneous oral or written communications, proposals and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment or similar communications between the parties. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software. The disclaimers of warranties and damages and limitations on liability shall survive termination. Software and documentation is delivered Ex Works California, U.S.A. or Dublin, Ireland respectively (ICC INCOTERMS 2000). This Agreement may only be modified by a License Module which accompanies this license or by a written document which has been signed by both You and Symantec. Should You have any questions concerning this Agreement, or if You desire to contact Symantec for any reason, please write to: (i) Symantec Customer Service, 555 International Way, Springfield, OR 97477, U.S.A., (ii) Symantec Customer Service Center, PO BOX 5689, Dublin 15, Ireland, or (iii) Symantec Customer Service, 1 Julius Ave, North Ryde, NSW 2113, Australia.

Contents

ManHunt Smart Agent for Symantec™ Host IDS 4.1 1
System requirements 1
Installation overview 2
Installing the MSA for Symantec Host IDS 4.1 2
Configuring the SESA Management 6
Installing the Symantec Host IDS 4.1 meta data 8
Configuring Symantec ManHunt 10

ManHunt Smart Agent for Symantec™ Host IDS 4.1

The ManHunt Smart Agent (MSA) for Symantec Host IDS 4.1 enables Symantec ManHunt to receive events in real time from the Symantec Enterprise Security Architecture (SESA) Manager. ManHunt then converts these events into the ManHunt event format, and sends the events to a ManHunt node for aggregation, correlation, and reporting, with all other ManHunt events. The MSA also enables you to set response policies for Symantec Host IDS events in the ManHunt Policy Configuration interface. (See *Symantec ManHunt Administration Guide* for instructions on creating response policies.)

System requirements

The MSA for Symantec Host IDS 4.1 requires the following:

- Symantec Host IDS 4.1 running on Windows 2000 Professional with Service Pack 2.
- SESA Manager 1.1 running on Windows 2000 Server.
- Symantec ManHunt 2.2 patch 2 installed on Solaris 8 SPARC or Intel, or Symantec ManHunt 3.0 installed on Solaris 8 SPARC or Intel, or Red Hat® Linux® 8.0 (with kernel version 2.4).

Note: Patch 2 is required for ManHunt 2.2 to enable you to properly view event information from MSAs. You can download the patch at: http://www.symantec.com/techsupp/enterprise/products/manhunt/manhunt_2.2/files.html.

To find out which ManHunt patches have been installed, look in the <ManHunt_inst_root>/patchlevel file. The content of the patchlevel file will include the entry `1:2.220.02:ManHunt patch 2.220.02` if you have patch 2 installed. If you do not have a patchlevel file, no patches have been installed.

Installation overview

The MSA for Symantec Host IDS 4.1 can be set up in six basic steps.

To set up the MSA for Symantec Host IDS 4.1

1. Ensure that you have installed Symantec ManHunt 2.2 patch 2, or Symantec ManHunt 3.0.
2. Install the MSA for Symantec Host IDS 4.1.
   See "Installing the MSA for Symantec Host IDS 4.1" on page 2.
3. Configure the Symantec management console.
   See "Configuring the SESA Management" on page 6.
4. Install the Symantec Host IDS 4.1 meta data on the ManHunt node.
   See "Installing the Symantec Host IDS 4.1 meta data" on page 8.
5. Configure Symantec ManHunt for Symantec Host IDS 4.1.
   See "Configuring Symantec ManHunt" on page 10.

Installing the MSA for Symantec Host IDS 4.1

You must install the MSA for Symantec Host IDS 4.1 on the SESA Manager host from which you want to receive events. If multiple SESA Managers are using the same SESA database, the MSA for Symantec Host IDS 4.1 must be installed on each SESA Manager to enable events to be sent to ManHunt.

The MSA for Symantec Host IDS 4.1 receives the Symantec Host IDS 4.1 event data, converts the data into the ManHunt event format, and sends the converted data to the ManHunt node. During the MSA installation, you specify the IP address of the ManHunt node that will receive the event data from the MSA. The MSA and ManHunt node communicate over Event Dispatch Protocol (EDP). To ensure secure and encrypted communication over EDP, they must share an EDP passphrase.

Note: You must be logged in as root to run the install script.

To install the MSA for Symantec Host IDS 4.1

1. Place the CD in the CD-ROM drive of the SESA Manager host.
2. Change to the CD directory, and type the following command:

   `Shids41MSA_MH<version>/java -jar setup.jar`

   where `<version>` is `22` or `30`

   You can change how the installation runs by passing one of the following arguments to the executable:

`-debug`	Prints debug information and also creates a SIPIInst.log file in C:\Documents and Settings\<username>\Local Settings\Temp\ with all the debug information.
`-silent`	Runs the SESA Integration Wizard silently (requires the indicated arguments).
`-userDN <userdn>`	User name used to connect to the SESA directory (required for -silent).
`-password <password>`	Password used to connect to the SESA directory (required for -silent).
`-sesaDirectory <hostname>`	Machine host name or IP address of the SESA directory (required for silent).
`-sesaDirectoryPort <port>`	Port number of the SESA directory (required for silent). Usually 636.
`-info`	Displays all information regarding the SESA Integration Wizard, including version and point product information packaged in the Wizard.
`-help`	Displays all available arguments.
`-uninstall`	Runs the SESA Integration Wizard in uninstall mode. This will completely delete the schema installed by the point product, both from the SESA directory and the SESA database. All events logged by that point product will be deleted. It is recommended to delete or archive those events before uninstalling.

3. In the SESA Integration Wizard, click Next twice.

4 In the SESA Domain Information Window, type the following information about the SESA Domain Administrator and SESA directory:

SESA Domain Administrator	The name of the SESA directory Domain Administrator account
SESA Domain Administrator Password	The password for the SESA directory Domain Administrator account.
IP Address of SESA Directory	The IP address of the computer on which the SESA directory is installed.
SSL Port	The number of the SESA directory secure port. By default, 636.

Note: This step is not necessary if you have already typed in this information at the command line.

5 Click Next twice and then click Finish to complete the install.

If you are running Symantec Host IDS you will have to restart the SESA console before the MSA will appear.

Symantec Host IDS 4.1 to ManHunt event severity mapping

The default reliability setting of Symantec Host IDS 4.1 events is 128 (medium), and the severity mapping from Symantec Host IDS 4.1 to ManHunt is as follows:

Table 1-1 Symantec Host IDS 4.1 to ManHunt severity mapping

Symantec Host IDS Event Severity	Range	ManHunt Event Severity	Range
Informational	0	Informational	0
Informational	0-6	Low	1-16
Informational	7-12	Medium	17-32
Informational	13-24	High	33-61
Warning	25-28	High	62-72
Warning	29-37	Urgent	73-96
Warning	38-47	Critical	97-120
Warning	48-59	Fatal Error	121-150
Critical	60-100	Fatal Error	151-255

Uninstalling the MSA for Symantec Host IDS 4.1

Except for the initial command, the process to uninstall the MSA for Symantec Host IDS 4.1 is identical to the installation process.

To uninstall the MSA for Symantec Host IDS 4.1

1. Place the CD in the CD-ROM drive of the SESA Manager host.
2. Change to the CD directory, and type the following command:

   `Shids41MSA_MH<version>/java -jar setup.jar -uninstall`

   where <version> is 22 or 30

   The script will ask if you wish to continue uninstalling the MSA.
   See "Installing the MSA for Symantec Host IDS 4.1" on page 2.

Note: If, after installing the MSA for Symantec Host IDS 4.1 meta data, you require more space on the disk, manually remove the meta data by deleting the Symantec_Host_IDS-policy.md file and the Symantec_Host_IDS-events.md file from the <ManHunt_install_directory>/md/ directory.

See "Installing the Symantec Host IDS 4.1 meta data" on page 8.

Configuring the SESA Management

You must configure the MSA for Symantec Host IDS 4.1 and its corresponding SESA Agent in the Symantec management console. The following sections describe this processes:

- Configuring the MSA for Symantec Host IDS 4.1
- Configuring the SESA Agent
- The MSA relay status page

Configuring the MSA for Symantec Host IDS 4.1

This section describes how to configure the MSA for Symantec Host IDS 4.1 in the Symantec management console.

To configure the MSA for Symantec Host IDS 4.1

1. Click the Configurations tab in the Symantec management console.
2. Click MSA for Symantec Host IDS > ManHunt Event Relay > Default.
   In the right window pane click the MSA Settings tab and enter the following information:

Table 1-2 MSA Configuration Parameters

Parameter	Description
ManHunt IP address	IP address of the ManHunt node to which you want to forward Symantec Host IDS events.
ManHunt EDP port	The ManHunt EDP (Event Dispatch Protocol) port. By default, 1333.
ManHunt EDP secret	The ManHunt EDP passphrase.
ManHunt Relay Log Level	The level of logging of Symantec Host IDS events sent to ManHunt via the MSA. There are 3 values: ■ Low—only error events will be sent. ■ Medium—all events sent will be logged, but only those fields the MSA passes to ManHunt will be logged (these are: Event type, Destination IP, and Text Data) ■ High—all events will be logged and all Symantec Host IDS fields for those events will be logged. The log file will be stored in C:\Program Files\IBM Http Server\tomcat\webapps\ManhuntRelay\ or, if you have installed IBM HTTP Server and tomcat in a different directory, C:\<tomcat install directory>\webapps\ManhuntRelay\.

Configuring the SESA Agent

This section describes how to configure the SESA Agent in the Symantec management console. Realize that the MSA for Symantec Host IDS 4.1 will start and stop as you start and stop the SESA Agent on the Symantec management console. See *Symantec Enterprise Security Architecture Administration Guide* for details.

To configure the SESA Agent

1. Click the Configurations tab in the Symantec management console.
2. Click SESA > SESA Agent Configuration > Default.
3. In the right window pane, click the Configuration tab.
4. Set the Config poll time property to 1 minute.
5. Click Apply.

Caution: Changing other SESA Agent configuration parameters may lead to degraded or unpredictable performance of the MSA. In particular, the App Flush Size setting should always be left at the default value of 50 kb, or considerable delays in event forwarding from SESA will occur.

The MSA relay status page

The MSA relay status page allows you to view statistics on events sent to ManHunt via the MSA for Symantec Host IDS, as well as configuration settings for the MSA. This page can be viewed at: https://<IP address of your SESA machine>/ManhuntRelay/servlet/ManhuntRelay/.

Note: Accessing the relay page requires the SESA domain administrator name and password.

Installing the Symantec Host IDS 4.1 meta data

You must install the Symantec Host IDS 4.1 meta data on the ManHunt node that you log into from the administration console, typically the primary master node. This is done in order for you to be able to create the MSA for Symantec Host IDS 4.1 external sensor node, create response policies for Symantec Host IDS 4.1 events, and display Symantec Host IDS 4.1 event data in the ManHunt console.

In addition, you must install this meta data on the ManHunt node that will receive the Symantec Host IDS 4.1 event data from the MSA for Symantec Host IDS 4.1 (if different from the master node).

Note: You must be logged in as root to install the Symantec Host IDS 4.1 meta data.

To install the Symantec Host IDS 4.1 meta data

1. Place the CD in the CD-ROM drive of the Symantec ManHunt host; mount the volume if necessary.
2. Change to the CD directory and enter the install command:

   `cd Shids41MSA_MH<version>/install/<platform>`

   where `<version>` is `22` or `30`, and `<platform>` is `linux`, `solaris8-intel`, or `solaris8-sparc`.

   `./install-md.sh`
3. Ensure that the meta data file to be installed begins with 'Symantec_Host_IDS' and ends with the '.md' file extension. If you have old meta data files, you can choose to either delete or archive them.

   Do one of the following:

   - Type `delete` and press Enter to delete the old meta data files.
   - Type `archive` and press Enter to archive the old meta data files.
4. ManHunt must be restarted to incorporate the new meta data.

   Type `y` and press Enter when prompted to restart ManHunt. If this is the ManHunt node used for administration, quit and restart any administration consoles connected to the node to enable the consoles to incorporate the new meta data.

As Symantec releases new policies for Symantec Host IDS via LiveUpdate, it will be necessary to install a new metadata file. You can find information on the latest Symantec product updates at http://www.symantec.com/avcenter/.

Note: If, when uninstalling the MSA for Symantec Host IDS 4.1 you require more space on the disk, manually remove the meta data by deleting the Symantec_Host_IDS-policy.md file and the Symantec_Host_IDS-events.md file from the <ManHunt_install_directory>/md/ directory. See "Uninstalling the MSA for Symantec Host IDS 4.1" on page 5.

Configuring Symantec ManHunt

You must configure Symantec ManHunt to enable communication between ManHunt and the MSA for Symantec Host IDS. The following sections describe how to configure ManHunt:

- Adding an external sensor node
- Adding an interface to an external sensor node
- Changing the EDP passphrase

Adding an external sensor node

To set ManHunt response policies for Symantec Host IDS events, you must add an external sensor node in the ManHunt topology tree for the machine on which the MSA for Symantec Host IDS 4.1 is installed.

To add an external sensor node

1. Open the ManHunt console.
2. Right-click External Sensors in the topology tree, and click Add External Sensor in the pop-up menu.
   The Add External Sensor dialog appears.
3. Enter a name of up to 39 characters for the device.
   This name will appear in the topology tree.
4. Enter an optional customer ID.
   This ID is a way of labeling the devices, for example, to describe the physical location of the device.
5. Enter the IP address for the SESA machine on which you installed the MSA for Symantec Host IDS 4.1.
6. From Smart Agent Type, choose one of the following:
   - For Symantec ManHunt 2.2, choose Symantec_Host_IDS
   - For Symantec ManHunt 3.0, choose Symantec Host IDS.

   Note: The Symantec Host IDS 4.1 Smart Agent type only appears in the drop-down list if you have installed the Symantec Host IDS 4.1 meta data.
7. Select the ManHunt node that will receive event data from the MSA for Symantec Host IDS 4.1.

Note: You must select the ManHunt node before setting the EDP passphrase, as ManHunt sets the EDP passphrase for the ManHunt node that is selected in the Event Receiver box at the time that you enter the EDP passphrase.

8. Set the EDP passphrase.

   This passphrase must be the same passphrase you entered during the MSA for Symantec Host IDS 4.1 installation process.

9. Enter a description for the MSA for Symantec Host IDS 4.1.

   This description will be displayed on the main console screen when this external sensor node is selected in the topology tree.

10. Click OK, then click Topology > Save Changes to save your topology tree changes.

Adding an interface to an external sensor node

The MSA for Symantec Host IDS 4.1 can take input from more than one source. You may add a description to each interface that corresponds to the external sensor you added in the ManHunt console. This allows for better correlation and presentation of Symantec Host IDS 4.1 events in the ManHunt console.

Note: You may add an interface to an external node in Symantec ManHunt 3.0 only.

To add and interface to an external sensor node

1. Right click on the external sensor you added for the MSA for Symantec Host IDS 4.1 in the ManHunt console, and click Add Interface in the pop-up menu.

   The Add MSA Interface dialog appears.

2. Enter a name of up to 39 characters for the interface.

   This name will appear in the topology tree.

3. Enter an optional customer ID.

   This ID is a way of labeling the source, for example, to describe the physical location of the sensor.

4. Enter the IP address for the machine on which you installed the device.

5. Enter the netmask.

6 Enter a description for the device.

This description will be displayed on the main console screen when this external sensor node is selected in the topology tree.

7 Click OK, then click Topology > Save Changes to save your topology tree changes.

Changing the EDP passphrase

To change the EDP passphrase on the ManHunt node, edit the external sensor topology tree node. The EDP passphrase on the ManHunt node must match the EDP passphrase on the MSA for Symantec Host IDS 4.1 machine. Therefore, if you change the passphrase on the ManHunt node, you must also change the passphrase on the MSA for Symantec Host IDS 4.1 machine by running the changesecret command located in the <MSA_install_directory>/bin directory.

To change the EDP passphrase on the ManHunt node

1 Log into the ManHunt console.

2 Right-click the appropriate external sensor node, and select Edit.

The Edit External Sensor dialog appears.

3 Click Set EDP Passphrase.

The EDP Passphrase dialog appears.

4 Enter the new passphrase the ManHunt node will use to communicate with the MSA for Symantec Host IDS 4.1.

This passphrase must be at least 8 characters long.

5 Re-enter the passphrase for confirmation.

6 Click OK, then click OK in the Edit External Sensor dialog box.

7 Click Topology > Save Changes.